What is Claimed Is:

1. A digital file forming a contract comprising:

a header package having rules defining sealed packages produced by a sealing party;

a body containing at least a portion of the content of the contract; and a validating signature generated from said rules and said body according to a first key belonging to a validating party; and

a sealing signature generated from said header package and said sealed packages according to a second key belonging to said sealing party.

2. A digital file forming a contract according to claim 1 wherein said header package further comprises a unique header identifying a type of said sealed package and wherein said validating signature is generated from said rules, said body and said header.

3. A digital file forming a contract according to claim 1 wherein said sealed package comprises a unique number generated by said sealing party and said sealing signature is generated from said header package, any of said sealed packages and said unique number.

4. A digital file according to claim 1 wherein said rules define one or more unsealed packages to be included in said sealed package, said body comprises a HTML file and one of the unsealed packages defined in the rules contains data for a field in the HTML file.

5. A digital file according to claim 1 wherein said rules comprise a URL corresponding to the location for which each sealed package to be included in the contract

can be obtained.

6. A digital contract according to claim 5 wherein said URL is a CGI script for commanding a remote server to generate said sealed package.

7. A digital contract according to claim 5 wherein said URL identifies the location of said sealed package.

8. A contract management apparatus for validating a digital file constituting a contract, said digital file having a header package which includes rules defining sealed packages, a body containing at least a portion of the contract, and a validating signature, comprising:

means for reading said rules and for identifying a validating party and a sealing party which created a sealed file of said contract;

first means for obtaining a first key belonging to said validating party cooperable with said validating signature generated from said rules and body to validate said header package;

second means for obtaining a second key belonging to said sealing party cooperable with said sealing signature to validate said contract; and

means for iteratively validating any sealed packages contained in said contract using said second key and sealing signature.

9. A contract management apparatus as claimed in claim 8 wherein said iterative validating means returns any data stored in said sealed packages.

10. The contract management apparatus of claim 9 further comprising means for displaying said body contents and said returned data.

11. A contract management apparatus for generating a digital file constituting a contract comprising:

means for obtaining a header package for said contract;

means for reading rules defining sealed data packages, and for identifying a sealing party and any sealed packages to be included in said contract;

means for obtaining said identified sealed packages;

means for generating a sealing signature from said header package and any of said sealed packages according to a first key belonging to said sealing party; and

means for assembling said header package, sealed packages and said sealing signature into said digital file constituting a contract.

12. A contract management apparatus comprising:

means for accepting and securely storing data files constituting contracts in an encrypted package database;

means for backing-up said package database;

a navigator tool adapted to allow a user access to said stored data files constituting said contracts;

means, responsive to a request for an encrypted package from said data base, for transmitting said package to an external entity;

means for informing users of data files having expiring contracts in said data base; and

means for deleting contracts from said data base.

13. The contract management apparatus of claim 8, including one of a smartcard, a personal digital assistant, a personal computer, a terminal or an embedded system.

14. A computer product for storing instructions which are executed by a computer to validate a digital file having a header package which includes rules defining sealed packages, a body containing at least a portion of a contract and a validating signature, comprising:

reading said digital file and identifying a validating party and a sealing party which created a sealed package of said contract;

deriving a first key belonging to a validating party;

validating said header package using said first key and said validating signature;

deriving a second key belonging to said sealing party;

deriving a sealing signature from said header package; and

validating said digital file using said second key and said sealing signature.

15. The computer product according to claim 14, further comprising instructions for deriving said sealing signature from a unique number contained in said header package.

16. A computer product storing instructions for execution on a computer to perform a process to validate a digital file constituting a contract comprising the steps of:

unzipping a header package in said digital file and reading rules contained in said header package;

determining from said rules keys to validate said header package and a sealed package of said digital file constituting said contract; and

validating each sealed package in said digital file using said keys.

17. The computer product storing instructions for execution on a computer

according to claim 16, further comprising instructions for performing the additional steps of obtaining said keys from a network server identified by said rules.

18. A computer product for storing instructions for a computer to execute the process comprising the steps of:

storing rules to describe a data package;

creating from said rules a data package containing a digital data file;

merging said rules and said data package into a merged file;

creating a package validity signature from said merged file to prevent unauthorized use of said digital file; and

generating a unique number identifying said digital file;

merging said package validity signature, said merged file and said unique number;

creating a sealing signature from said merged files; and

sealing said merged files with said sealing signature to produce a sealed package.

19. A computer product according to claim 18 wherein said rules comprises a plurality of elements which point to a location on said computer containing a required package.

20. The computer product according to claim 19 wherein said rules define a sealing signature for said sealed package.

21. The computer product according to claim 18 wherein said merged files are compressed as a single file.